Naval Research Laboratory

Washington, DC 20375-5320

NRL/MR/5542--07-9084

The Protections of Bilaterally Sensitive Information on a Restricted Multilateral Network

Myong Kang

Center for High Assurance Computer Systems
Information Technology Division

Steven Pieper

Command, Control, Communications, Computers, and Intelligence Branch
Space Systems Development Department

Jeremy Smith
Allen Yeh

Assurance Technology Corporation
Alexandria, Virginia

October 19, 2007

Approved for public release; distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 19-10-2007	**2. REPORT TYPE** Memorandum Report	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE

The Protections of Bilaterally Sensitive Information
on a Restricted Multilateral Network

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Myong Kang, Steven Pieper, Jeremy Smith,* and Allen Yeh*

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

55-9103-G-7

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Naval Research Laboratory, Code 5542 and Code 8143
4555 Overlook Avenue, SW
Washington, DC 20375-5320

8. PERFORMING ORGANIZATION REPORT NUMBER

NRL/MR/5542--07-9084

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Office of the Secretary of Defense, Advanced Systems and Concepts, The Pentagon
Army Navy Dr. and Fern St.
Arlington, VA 22202

10. SPONSOR / MONITOR'S ACRONYM(S)

11. SPONSOR / MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

*Assurance Technology Corporation, Alexandria, VA 22307

14. ABSTRACT

Historically, fully separate technical implementation was required for each bilateral information exchange, which is largely supported by the U.S. in terms of facilities, manpower, and infrastructure at substantial cost. In this report, we propose a solution that will allow the U.S. to consolidate some of these networks while assuring that information will be treated with the appropriate degree of confidentiality.

15. SUBJECT TERMS

Multilateral network
Coalition network
Label security

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Myong H. Kang
a. REPORT Unclassified	**b. ABSTRACT** Unclassified	**c. THIS PAGE** Unclassified	UL	12	**19b. TELEPHONE NUMBER** *(include area code)* (202) 767-3654

The Protections of Bilaterally Sensitive Information On a Restricted Multilateral Network

White Paper Prepared by the Naval Research Laboratory in coordination with COMPACFLT

Myong Kang and Steven Pieper
Naval Research Laboratory
Washington DC 20375

Jeremy Smith and Allen Yeh
Assurance Technology Corporation
Alexandria VA 22307

Introduction

The United States has identified the importance of facilitating international military cooperation to support increased security, the mitigation of mutual threats from states and non-state actors, coalition warfare, operations of humanitarian assistance, and maintenance and improvement of persistent situational awareness. These objectives have been accomplished through a variety of technical and non-technical means. There have been large differences between the implementations of technical solutions between nations, agencies, military services and theaters.

As a result of diplomatic intricacies the US may enjoy close relations with several nations, but those nations may not necessarily share the same degree of trust with each other. The need for a system to provide a means to guarantee good stewardship of sensitive information from each international source is of paramount concern in order to preserve the nature of international cooperation on large and complex operational needs.

Historically this has tended to require fully separate technical implementations for each bilateral exchange, which are largely supported by the US in terms of facilities, manpower, and infrastructure at substantial cost. Notable exceptions include the North Atlantic Treaty Organization (NATO) and other multinational alliances, which are supported by large multi-lateral Community of Interest (COI) networks. In recent years efforts have been under way to increase the number of nations participating in multilateral secure communications, but the information that can be exchanged over these networks must be determined to be releasable to all. Fielded examples have included the Coalition Enterprise Regional Exchange System (CENTRIXS) networks (GCTF, CFE, K, J, CMFP, CNFC, etc.), the networks supporting NATO, and there is a continuing effort within DISA to deliver the Multi-National Information Sharing (MNIS) solution.

A policy is needed to determine technical requirements for supporting maximum releasability of information in these environments. For this paper, the Naval Research Laboratory (NRL) assumes that need-to-know and separation-of-duties protections are acceptable to separate bilateral and reduced COI exchanges for the larger secured multilateral networks. This assumption will need to be validated in policy and international agreement.

The purpose of this paper is to propose a solution that will allow the US to consolidate some of these networks, while maintaining the degree of assurance that information will be treated with the appropriate degree of confidentiality.

Manuscript approved August 31, 2007.

Requirement

The US Navy has a mutual interest with many international navies in the areas of:

- Coalition operations
- Denial of the maritime environment to terrorists and other hostile non-state actors
- Prevention of acts of piracy
- Protection of the waterways for commercial interests
- Prevention of human trafficking across the maritime environment
- Maintenance of a persistent situational awareness of the maritime domain
- Identification of anomalies and mitigation threats to national interests
- Mitigation of the damage results, and expediting recovery from disasters
- Supporting operations of humanitarian assistance

Technical solutions are currently in place to support many of these objectives and concept development is underway to improve many objectives within the Department of the Navy (DoN) and the Department of Defense (DoD). As previously discussed, these solutions are often bilateral or supporting a fairly small COI, requiring the US Navy (USN) to support several separate coalition networks, with complete duplication of servers, routers, switches and other infrastructure in globally distributed data centers ashore and afloat.

There is a continuing requirement to consolidate the infrastructure in a way that supports sensitivity of information (assigned by the US and international counterparts), maximizes releasability based upon the nations participating in exchange, and is flexible enough to support dynamic political environments. Operator efficiency is another key benefit of consolidation of the coalition networks. Operators with higher levels of access and greater coordination responsibility currently must perform their duties on several separate computers, each with a specific level of access and releasability. This often requires a human intermediary to relay information from one COI to another, or requires the implementation of Cross Domain Solutions (CDS). CDS require a great deal of time in accreditation, and are not flexible; they cannot be counted upon to deliver the type of agility the global political environment requires.

What is required is a means to secure information of varying releasability that can be processed, sorted, analyzed and distributed. At the same time ensuring that all data is only available to organizations, commands, agencies, and nations based upon restrictions imposed by the data contributor/owner.

Policy Direction and Instruction

In order for the USN to field any solution to the above stated requirement, the system must be designed in coordination with US National policy, and must be able to be communicated at some level of technical detail with international partners in order to provide assurance for the confidentiality of shared data. According to US Government policy, the DoD is required to protect classified information provided by another nation, and to prevent its subsequent disclosure:

> "E3.1.3.2. Specifically Prohibited Disclosures. The following types of classified information are specifically prohibited from disclosure:
>
> E3.1.3.2.1 Classified information officially obtained from a foreign government, except when the information has been conveyed by the government with express written consent to its further disclosure."[1]

For the purposes of this paper, NRL assumes that "need-to-know" protections will be determined to be adequate separation of data at the same classification, but requiring different levels of releasability. "Need-to-know" is defined as "the determination that certain information or classes of information are required by an individual, command, agency, office, or organization in order to perform their duly assigned duties." "Separation of Duties" is defined as "the means by which information is segregated from consumers without an appropriately vetted 'Need-to-know'." This denial of non-essential or unauthorized information can be focused on individuals within an organization (such as Privacy Act data being restricted from non-human resources personnel) or organizations (such as military restrictions against accessing Law Enforcement Sensitive (LES) data).

There must be a determination of need-to-share in order for an organization or an individual to be granted access. As international contributors remain the rightful owners of the data, the US is bound by its own policy to determine that third parties do not have sufficient need-to-know without express written consent (as cited in footnote 1). In order to provide an assurance of confidentiality, need-to-know information must be protected within an Automated Information System (AIS) from unauthorized disclosure. Policy for the transmission of data is:

> "E4A4: Enclave and Computing Environment
>
> ENCK-1 Encryption for Need-to-Know
>
> Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at minimum, with NIST-certified cryptography. This is in addition to ECCT (encryption for confidentiality – data in transit)."[2]

Due to the potential diplomatic consequences of spillage, NRL recommends that the best of the FIPS-approved standard encryption algorithms be employed to protect bi-lateral (or restricted COI) classified information exchanges. Currently this is AES-256[3], tested and certified to the FIPS 140-2 standards. The National Institute for Standards and Technology (NIST) provides minimum standards for security controls in information systems. "Separation of Duties" protections require:

> "Control:
>
> The information system enforces separation of duties through assigned access authorizations.
>
> Supplemental Guidance:
>
> […] There is access control software on the information system that prevents users from having all the necessary authority or information access to perform fraudulent activity without collusion. […]"[4]

[1] DoD Directive 5230.11, Page 21

[2] DoD Instruction 8500.2, Page 89

[3] Technical description of the algorithm can be found in FIPS 197

[4] NIST Special Publication 800-53, R1, Page 58 "AC-5"

These controls should apply to users or system components that will further ensure that information is not available inadvertently or maliciously to unauthorized users or organizations without the express aide of authorized users. NRL recommends that critical security system components are designed in accordance with DCID 6/3, and evaluated in accordance with the International Organization for Standardization ISO/IEC 15408 Common Criteria (CC) for computer security, and receive confirmation of Evaluation Assurance Level (EAL) 4 or greater.

Common Criteria:

> The CC permits comparability between the results of independent security evaluations. The CC does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software. [5]

Evaluation Assurance Level 4:

> EAL4 permits a developer to gain maximum assurance from positive security engineering. Based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.[6]

A Proposed Solution

Coalition partner nations are willing to share data with each other as long as they have an agreement to share data. The data from a country should not be shared with any other nations unless the data owner explicitly grants permission. To describe required system behavior, we will provide a few examples.

1. Country 1 has bilateral agreements to share data with countries 2, 3, 4, and 5.
2. Country 2 and country 3 do not have any agreement to share data between them.
3. Country 2’s data that resides in country 1’s system will not be disclosed to any users from country 3 (see figure 1).

To prevent unauthorized monitoring of information during exchange, all data transfer will be encrypted using specific keys pre-arranged for point-to-point connections. Assuming that all users are in the same level of network (i.e., normal network protocol works between a sender and a receiver), the security requirements that are being derived from the above statement are as follows:

- User authentication
- Confidentiality in the network
- Stateless applications so that they can be re-used among many users
- Separation of data and marking of the ownership in data storage
- Access control to the data based on user credentials and the origin of data
- Encryption of data as it is transited using authorized algorithms and keymat particular to each bi-lateral exchange

[5] CC for Information Technology Security Evaluation v3.1, Part 1, Page 9, Para 1

[6] CC for Information Technology Security Evaluation v3.1, Part 3, Page 38, Para 111

The main security mechanisms in the proposed solution are encryption in the network, federated authentication and authorization (Federated A&A) to honor autonomy of participating nations and to reduce the security risk, and Oracle Label Security (OLS) to separate data in the database.

The simplified architecture is shown in figure 1.

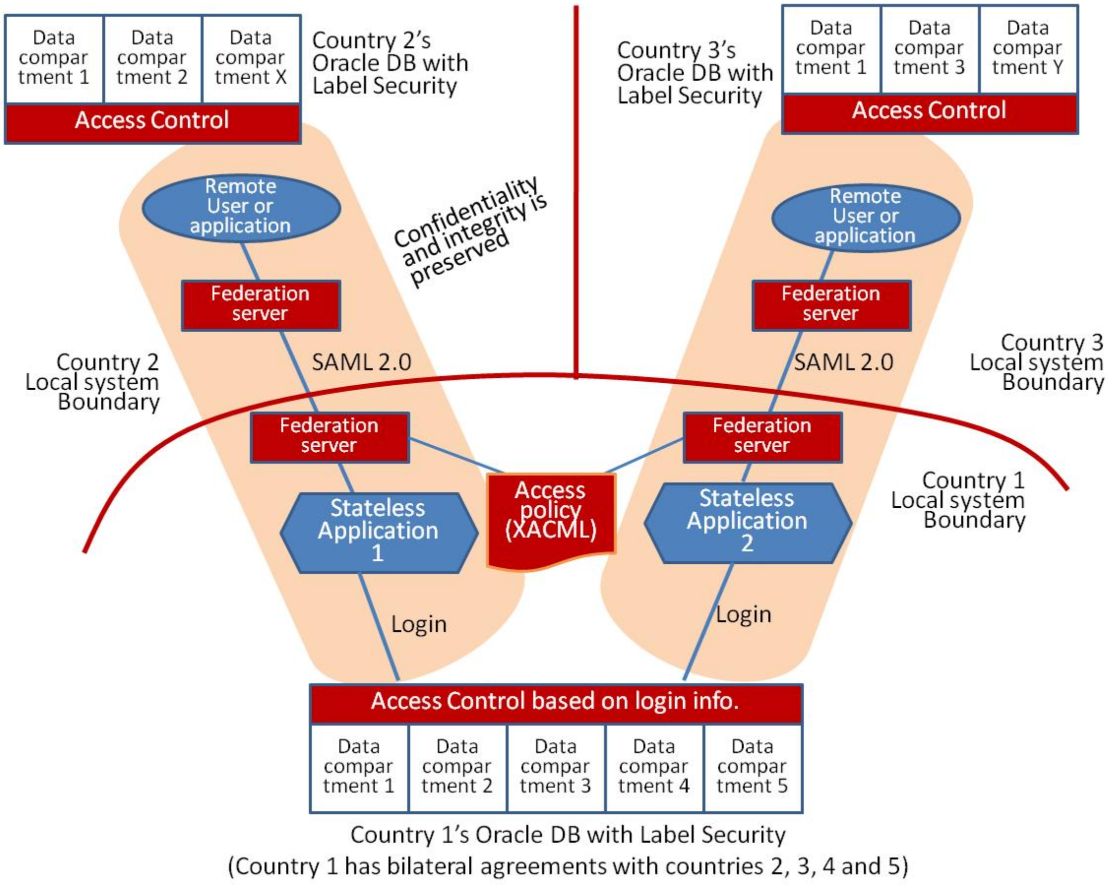
Data compar tment 1
Data compar tment 2
Data compar tment X
Country 2's Oracle DB with Label Security
Access Control
Country 3's Oracle DB with Label Security
Data compar tment 1
Data compar tment 3
Data compar tment Y
Access Control
Remote User or application
Confidentiality and integrity is preserved
Remote User or application
Federation server
Federation server
Country 2 Local system Boundary
SAML 2.0
SAML 2.0
Country 3 Local system Boundary
Federation server
Federation server
Access policy (XACML)
Stateless Application 1
Stateless Application 2
Country 1 Local system Boundary
Login
Login
Access Control based on login info.
Data compar tment 1
Data compar tment 2
Data compar tment 3
Data compar tment 4
Data compar tment 5
Country 1's Oracle DB with Label Security
(Country 1 has bilateral agreements with countries 2, 3, 4 and 5)

Figure 1- Simplified Architecture of the Proposed Solution for Bilaterally Sensitive Information on a Restricted Multilateral Network Environment

In this restricted multilateral network environment, the main data separation mechanism is Oracle Label Security. Oracle Database 10g Enterprise Edition and OLS have been evaluated at DCID 6/3 EAL 4+[7]. Thus, its security mechanism is quite robust in terms of enforcing security policy and separating data based on security labels. When the data from a partner nation arrives to the system, it is labeled according to the nation that provided it. For example, country 2 shares data with country 1, the data will be labeled as country 2.

Users cannot access the database directly. They will access the data through applications (or Web services). When a user (client) tries to access an application (service), they must authenticate themselves (specifically, a user authenticates to its own organization and the

[7] In this case the + signs indicate an augment beyond what is required for EAL 4 by adding additional assurance components

federation service takes care of the rest of the authentication process). The authentication protocol that we propose to use is Security Assertion Markup Language (SAML) 2.0 that is an OASIS standard. SAML 2.0 is the only standard that client and service organizations have to agree to. Specific implementations of SAML 2.0 can be chosen from independent vendors, designers, and integrators. This protocol assumes there is an established trust relationship between a client organization and a service organization. If there is no trust relationship, all SAML requests by a client will be rejected by the service organization. If a user has permission to access a service, execution of the service is granted. The service (or application) is stateless (i.e., does not retain any previous information) and does not know anything about the data labels. It behaves exactly the same way with all users. When the service accesses the database, it will utilize user authentication information for database login. Depending on the user, a different set of data will be returned to the service. For example:

- If a user from country 2 accesses country 1's service (see figure 1), the result will be based on the data from country 2 and country 1 because the database will return only country 2 and country 1 data to the service (i.e., country 2 and country 1 have bilateral agreement to share data).
- If a user from country 3 accesses country 1's service (see figure 1), the result will be based on the data from country 3 and country 1 because the database will return only country 3 and country 1 data to the service (i.e., country 3 and country 1 have bilateral agreement to share data).

As long as a user has a permission to use a service, user access to a service will be granted. However, the access control in the OLS will mediate data access based on data labels and user credential. For example:

- Only country 1 and country 2 personnel can access data in the country 2 compartment because only country 1 and country 2 have the bilateral agreement to share country 2's information.
- Users from other nations do not even know that there is a country 2 data in the system.
- If country 1 has a bilateral agreement with country 2 and another bilateral agreement with country 3, country 1 users can access data from country 1, country 2 and country 3. But country 2 will never have access to country 3 data and vice versa. Unless there is an agreement made at a later time.

Once authorization is assured, then the actual data will be transmitted across the network in an encrypted mode. Keying material maintenance responsibilities will need to be identified in the initial agreements between nations, and will need to be treated with the same level of sensitivity as the potential information that could transit the system as a whole. Transmissions such as database replications may require point-to-point connections between Network Operations Centers (NOCs) in several host nations. It is recommended that data exchanges between nations be performed by NOCs or regional nodes, who would forward information to national enterprises using a single-nation key. See the data transmission architecture in
Figure 2- Secured Information Exchange and Data Distribution Based Upon International Agreement.

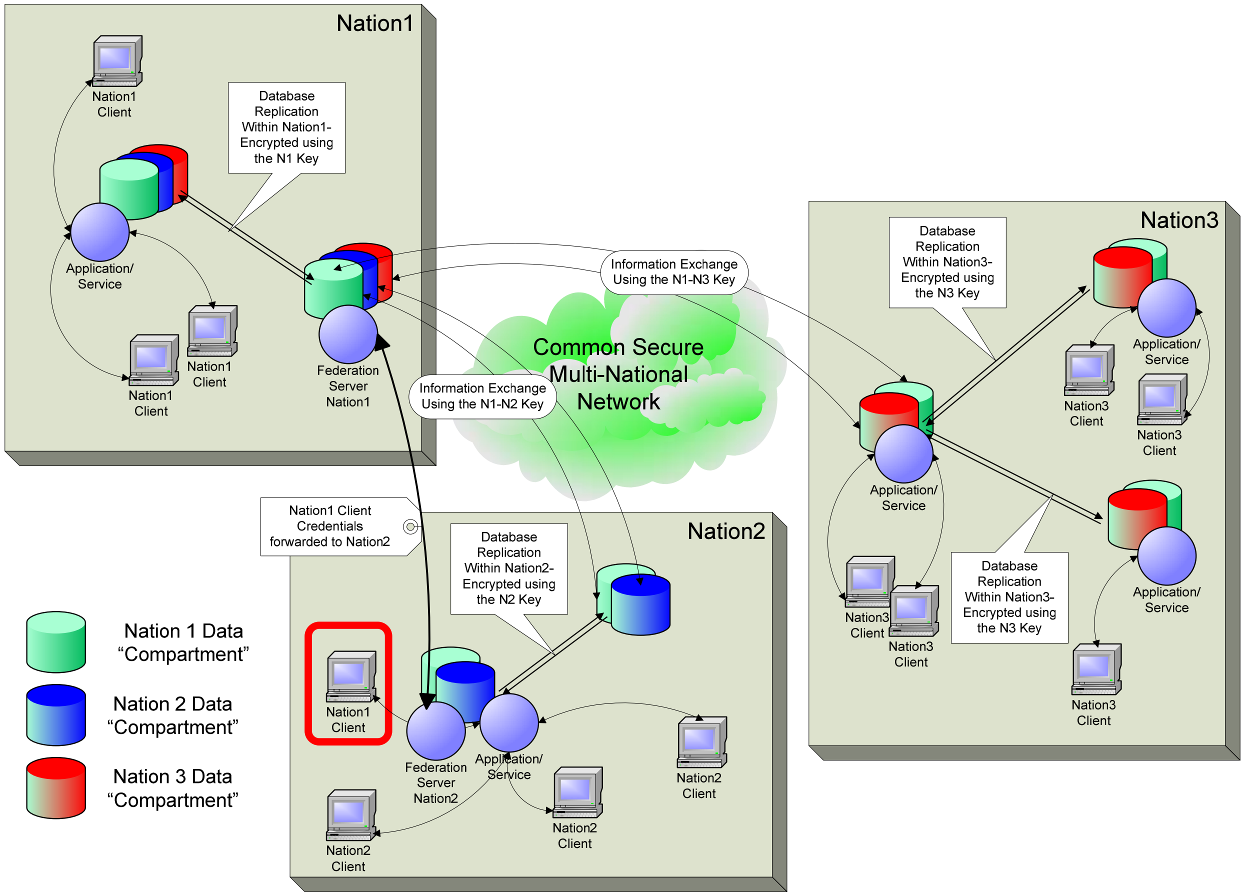
Nation1
Nation1 Client
Database Replication Within Nation1- Encrypted using the N1 Key
Application/ Service
Nation1 Client
Nation1 Client
Federation Server Nation1
Information Exchange Using the N1-N3 Key
Common Secure Multi-National Network
Information Exchange Using the N1-N2 Key
Nation3
Database Replication Within Nation3- Encrypted using the N3 Key
Application/ Service
Nation3 Client
Nation3 Client
Application/ Service
Nation3 Client
Nation3 Client
Database Replication Within Nation3- Encrypted using the N3 Key
Application/ Service
Nation3 Client
Nation1 Client Credentials forwarded to Nation2
Nation2
Database Replication Within Nation2- Encrypted using the N2 Key
Nation1 Client
Federation Server Nation2
Application/ Service
Nation2 Client
Nation2 Client
Nation2 Client
Nation 1 Data “Compartment”
Nation 2 Data “Compartment”
Nation 3 Data “Compartment”

Figure 2- Secured Information Exchange and Data Distribution Based Upon International Agreement

In the above example, there is an embedded user from Nation1 in a Nation2 workspace. Their credentials are forwarded using the SAML protocol for access to local host nation services and data. Embedded users of this type offer a specific challenge to the supporting system. While Nation1 has an agreement with both Nations2 and 3, Nation2 does not have an agreement with Nation3. A user from Nation1 is technically authorized to access services and applications that can build, fuse, associate or add other value to data from all three nations. In order to prevent the disclosure of data from Nation3 to Nation2 by a Nation1 embedded user, there needs to be a notion of context added to the security apparatus. Contextual constraints may include multinational facilities, military observers, visitors to a facility, etc. There should be an effective and simple means to sanitize a system to support changing locations of users and releasability levels of spaces.

In the specific example above, a user from Nation1 may access services (which access data) from either the local Nation2 data centers or the remote Nation1 data centers. In either case, his credentials need to forward his contextual information so that only the appropriate data is provided. Usually context is determined as an attribute of the physical computer that a user is logged into. Context can also be applied based upon login domains, identity management servers performing initial verification, or other logical means.

Assuming that a logical means is utilized to add context to a SAML assertion, it will be possible for the same arrangement to support sanitization of facilities when visitors are present. When incorporated with appropriate notification of human users this can be a very convenient means of attaining operational responsiveness. A single watch-floor could easily support scalable and fluid coalition operations with minimal reconfiguration.

Assurance

It is important to assure all parties that contributed data will be protected according to the agreement. Here is a rough sketch of assurance trail.

- All communication paths will be encrypted paths, thus, confidentiality and integrity of data on transit are assured.
- All applications will be stateless, thus, no information will be stored in the applications.
- Authentication is based on a chain of trust. First, users must authenticate themselves to local authority (e.g., local nation hosting the facility). Then the local authority provides an authentication assertion to a remote server site (e.g., remote nation hosting the service). Since the client site and the server site already established a trust relationship, the server site will accept the authentication assertion from the client site. The data access is based on the origin of data and the origin of an authentication assertion, users from one nation cannot access the data from other nations.
- The robustness of OLS security is CC EAL4+. Thus the data separation and access mediation mechanisms are robust.
- To ensure the Oracle access policies are encoded in a correct way. NRL plans to develop a tool that can extract all access policies from remote Oracle DBs and validate that users from one nation cannot access data from other nations unless authorized. This will be an open software product that is exchanged as part of the initial agreement between nations. This tool will allow all nations to monitor that their data is being treated in accordance with international agreement (forwarding, separation, protection, etc). This tool will interrogate the policies of all databases, and all parties will be required to permit queries and perform queries whenever they deem necessary.

Database Collaboration and Replication

Currently the USN has access to collaboration software/hardware suite, Lotus Notes/Domino which is already installed and used ashore and afloat in coalition environments. This system was implemented with system availability, security, and ease of use in mind. Any new implementations and deployments as suggested here would be intended as an augmentation to the systems previously fielded.

The database collaboration would be to take the Oracle database and cross connect it with a Lotus Domino database. Lotus Enterprise Integrator is a leading candidate to link these two databases so that they may transmit and receive information efficiently (see Figure 3). Lotus Enterprise Integrator will allow seamless transmission between the Oracle database and the Lotus Domino database. Lotus Enterprise Integrator and Lotus Notes/Domino will both retain the label security and authentication criteria as set forth previously in this document.

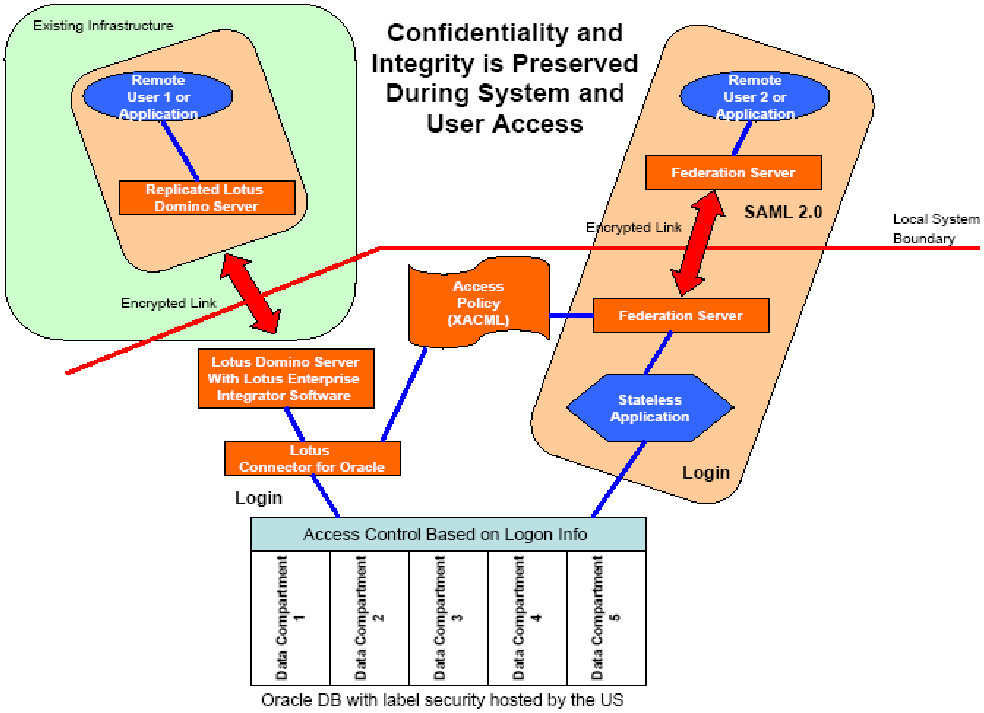
Existing Infrastructure
Remote User 1 or Application
Replicated Lotus Domino Server
Encrypted Link
Confidentiality and Integrity is Preserved During System and User Access
Remote User 2 or Application
Federation Server
SAML 2.0
Encrypted Link
Local System Boundary
Access Policy (XACML)
Federation Server
Stateless Application
Login
Lotus Domino Server With Lotus Enterprise Integrator Software
Lotus Connector for Oracle
Login
Access Control Based on Logon Info
Data Compartment 1
Data Compartment 2
Data Compartment 3
Data Compartment 4
Data Compartment 5
Oracle DB with label security hosted by the US

Figure 3- Collaboration architecture between Lotus Notes/Domino and Oracle DB

Conclusion

This white paper is intended to demonstrate that a fairly simple implementation of tested and validated systems can be completely consistent with existing policy and meet existing needs of the USN and DoD. The proposed solution allows the USN to consolidate some of its active networks, thereby reducing the DOTMLPF impacts of mission performance.

Clearly, US policy concerns and a security-minded implementation of these protections are only a part of the solution. Coalition members and allies will still need to validate, and accept these implementations as being sufficient to protect their national interests; but current precedent exists in exercise and demonstrations that this type of arrangement is diplomatically possible as long as frank and honest discussion of mutual security concerns can be conducted and resolutions addressed in a mutually beneficial manner.

References

a) Department of Defense Directive 8500.1, “Information Assurance,” October 24, 2002

b) Department of Defense Directive 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003

c) Department of Defense Directive 5230.11, Disclosure of Classified Military Information to Foreign Governments and International Organizations,” June 16, 1992

d) Secretary of the Navy Instruction 5510.31c, “Policy and Procedures for the Control of Foreign Disclosure in the Department of the Navy,” 15 March 2000

e) Defense Information Systems Agency Applications Security Project, “Security Requirements Methodology for Software Applications and Web Services,” July 15, 2004

f) NIST Special Publication 800-21, “Guideline for Implementing Cryptography In The Federal Government,” December 2005

g) Common Criteria for Information Technology Security Evaluation v3.1, “Part 1: Introduction and general model”, September 2006

h) Common Criteria for Information Technology Security Evaluation v3.1, “Part 3: Security assurance components”, September 2006

i) Federal Information Processing Standards (FIPS) Publication 199, “Standards for Security Categorization of Federal Information and Information Systems,” February 2004

j) FIPS Publication 197, “Advanced Encryption Standard,” November 26, 2001

k) FIPS Publication 200, “Minimum Security Requirements for Federal Information and Information Systems,” March 2006

l) ISO/IEC 15408-1:2005, “Common Criteria for Information Technology Security Evaluation- Part 1: Introduction and General Model,” 2005

m) ISO/IEC 15408-2:2005, “Common Criteria for Information Technology Security Evaluation- Part 2: Security Functional Requirements,” 2005

n) ISO/IEC 15408-3:2005, “Common Criteria for Information Technology Security Evaluation- Part 3: Security Assurance Requirements,” 2005